UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/820,666	04/08/2004	Geoffrey Dunbar	MSFT-2868/306927.1	8014

41505 7590 02/05/2007

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/820,666	DUNBAR ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/18/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 are presented for examination.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-16 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-23 of copending Application No. 10/820673. Although the conflicting claims are not identical, they are not patentably distinct from each other because the application '673 teaches all the claims limitation except the differences that are underlined in the following table as an example:

Instant application 10/820666	Copending application 10/820673
1. A method of delivering content from a source to a sink by way of a computing device, the method comprising: • an application on the computing device calling to a media base on the computing device with a definition of the content, the source, and the sink; • the media base establishing a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path including: • the media base; • a source trust authority (SOTA) associated with and corresponding to the source, the SOTA acting as a secure lockbox connecting the source to the media base and representing the source in the protected media path; and • a sink trust authority (SITA) associated with and corresponding to the sink, the SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path; • the SOTA on behalf of the source establishing trust with respect to the protected media path; • the SOTA upon trust being established with respect to the protected media path	12. A method of delivering content from a source to a sink by way of a computing device, the method comprising: • an application on the computing device calling to a media base on the computing device with a definition of the content, the source, and the sink; • the media base establishing a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path including: • the media base; • a source trust authority (SOTA) associated with and corresponding to the source, the SOTA acting as a secure lockbox connecting the source to the media base and representing the source in the protected media path, decrypting the content from the source if necessary, and translating policy associated with the content from a native format into a format amenable to the policy engine if necessary; and • a sink trust authority (SITA) associated with and corresponding to the sink, the SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path, encrypting content to be delivered to the sink if necessary, and translating the policy associated with the content from the format of the policy engine into a format amenable to the sink if necessary, whereby the sink receives the content and

propagating policy corresponding to the content to be delivered to the protected media path; • the SOTA determining a particular type of action to be taken with the content as delivered through the protected media path; • the SOTA deciding with regard to the propagated policy that the particular type of action cannot be taken with the content as delivered through the protected media path and informing the media base of a refusal to take such action; • the media base informing the application of the refusal to take the action; • the SOTA recognizing that the refusal may be rectified by way of a particular enabler available to such SOTA and the SOTA providing the particular enabler to the application by way of the media base, the provided enabler including information and methods necessary for the application to obtain data necessary to respond to the refusal; • the application receiving the enabler at an interface thereof by way of the media base, and the interface applying a common interaction procedure to run the enabler to obtain the data necessary to respond to the refusal; • the application providing the	corresponding policy, decrypts the received content if necessary, and renders same based on the received policy; • the SOTA on behalf of the source establishing trust with respect to the protected media path; • the SOTA upon trust being established with respect to the protected media path propagating policy corresponding to the content to be delivered to the protected media path; • the SOTA determining a particular type of action to be taken with the content as delivered through the protected media path; • the SOTA deciding whether the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same; • the media base informing the application whether the particular type of action can be taken, and if so the application proceeding by commanding the media base to perform such type of action. 19. The method of claim 18 wherein if the policy engine determines that a particular element of the protected media path does not satisfies the policy, the policy engine performs an action selected from a group consisting of refusing such element access to the content and preventing content from being delivered through the protected media path.

obtained data to the media base and the media base employing the provided data to respond to the refusal; • the SOTA deciding with regard to the propagated policy and based at least in part on the responded refusal that the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same; and the media base informing the application that the particular type of action can be taken, and the application proceeding by commanding the media base to perform such type of action.	

The differences between these two applications is that the instant application '666 has a narrower claim limitation as underlined above and the copending application has broader claim limitations and a secure lockbox act of decrypting/encrypting the content from the source, and translating policy associated with the content from a native format into a format amenable to the policy engine if necessary is not disclosed in '666 of claim limitations. Wherein said action, as described in the disclosure of the instant application, is an allowance and refusal action. The missing refusal action of claim 1 of the copending application is stated on dependent claim 19 of instant application. Regarding secure lockbox of decrypting/encrypting content is also described throughout the disclosure as being using a cryptography method to encrypt and lock contents.

Examiner applies, Stefik US 5,715,403 col. and col. 9 lines 58-60and col. 51 lines 24-31, for the well-known method of cryptography.

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of locking/encrypting method to secure and protect transmission of contents.

Claims 1-16 of the instant application are envisioned by copending Application No. '673 claims 1-23 in that claims 1-23 of the copending application contain all the limitations of claims 1-16 of the instant application. Claims 1-16 of the instant application therefore are not patently distinct from the copending application claims and as such are unpatentable for obvious-type double patenting.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Candelore USPN 7,120,250 B2.

Regarding claim 1, Candelore discloses a method of delivering content from a source to a sink by way of a computing device (fig. 1 and col. 4 lines 29-42), the method comprising:

an application on the computing device calling to a media base on the computing device with a definition of the content, the source, and the sink (fig. 1 and col. col. 4 lines 29-56);

the media base establishing a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path (col. 3 lines 35-59; DRM.... *encrypted communication*) including:

the media base (fig. 1; DRM);

a source trust authority (SOTA) associated with and corresponding to the source (fig. 1 element DRM A, B; *digital right management in the content provider system associated to every TV channel/webpage providers to protect digital contents*), the SOTA acting as a secure lockbox connecting the source to the media base (col. 4 lines 43-56; *connecting encrypted web contents and DRMs*) and representing the source in the protected media path (col. 4 lines 43-56; *connecting encrypted web contents and DRMs*); and

a sink trust authority (SITA) associated with and corresponding to the sink (fig. 7 element 722; *each user's usage content information detector/verifier in the DRM content provider system*), the SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path (fig. 7 element 742; *detector/verifier in the DRM content provider system allowing access to the end users from content provider system*);

the SOTA on behalf of the source establishing trust with respect to the protected media path (col. 6 lines 13-28; *DRM... copy rights protection on behalf of multiple different TV channels/web pages*);

the SOTA upon trust being established with respect to the protected media path propagating policy corresponding to the content to be delivered to the protected media path (fig. 7 element 722, and col. 4 lines 43-56);

the SOTA determining a particular type of action to be taken with the content as delivered through the protected media path (col. 6 lines 13-28; *viewing*);

the SOTA deciding with regard to the propagated policy that the particular type of action cannot be taken with the content as delivered through the protected media path and informing the media base of a refusal to take such action (col. 7 lines 41-65 and col. 6 lines 13-28; *deciding to allow/grant access based on usage term... limited time... keeping track of users access and recording and informing usage information to the DRMs of the content provider system*);

the media base informing the application of the refusal to take the action (fig. 7 element 726);

the SOTA recognizing that the refusal may be rectified by way of a particular enabler available to such SOTA (col. 4 lines 29-65 and col. 8 lines 16-39; *client updating terms/usage*) and the SOTA providing the particular enabler to the application by way of the media base (fig. 7 element 750), the provided enabler including information and methods necessary for the application to obtain data necessary to respond to the refusal (col. 7 lines 41-65);

the application receiving the enabler at an interface thereof by way of the media base, and the interface applying a common interaction procedure to run the enabler to obtain the data necessary to respond to the refusal (col. 7 lines 22-64);

the application providing the obtained data to the media base and the media base employing the provided data to respond to the refusal (col. 6 lines 13-28 and col. 7 lines 41-64);

the SOTA deciding with regard to the propagated policy and based at least in part on the responded refusal that the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same (fig. 7 element 726, and 750); and

the media base informing the application that the particular type of action can be taken, and the application proceeding by commanding the media base to perform such type of action (col. 7 lines 9-64).

Regarding claim 10, Candelore discloses a method of delivering content from a source to a sink by way of a computing device where an application on the computing device defines to a media base on the computing device the content, the source, and the sink, and the media base establishes a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path including the media base, a source trust authority (SOTA) associated with and corresponding to the source, the SOTA acting as a secure lockbox connecting the source to the media base and representing the source in the protected media path, and a sink trust authority (SITA) associated with and corresponding to the sink, the

SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path (fig. 1), the method comprising the SOTA:

establishing trust with respect to the protected media path (col. 6 lines 13-28; *DRM... copy rights protection on behalf of multiple different TV channels/web pages*);

upon trust being established with respect to the protected media path, propagating policy corresponding to the content to be delivered to the protected media path (fig. 7 element 722, and col. 4 lines 43-56);

determining a particular type of action to be taken with the content as delivered through the protected media path (col. 6 lines 13-28; *viewing*);

deciding with regard to the propagated policy that the particular type of action cannot be taken with the content as delivered through the protected media path and informing the media base of a refusal to take such action, where the media base informs the application of the refusal to take the action (col. 7 lines 41-65 and col. 6 lines 13-28; *deciding to allow/grant access based on usage term... limited time... keeping track of users access and recording and informing usage information to the DRMs of the content provider system*);

recognizing that the refusal may be rectified by way of a particular enabler available to such SOTA and providing the particular enabler to the application by way of the media base (fig. 7; elements 706, 718, 722, 750), the provided enabler including information and methods necessary for the application to obtain data necessary to respond to the refusal (fig. 7; elements 706, 718, 722, 750, and 726), where the application receives the enabler at an interface thereof by way of the media base (col. 7 lines 41-65), and the interface applies a common interaction procedure to run the enabler to obtain the data necessary to respond to the refusal (fig. 7 element

726), and where the application provides the obtained data to the media base and the media base employs the provided data to respond to the refusal (col. 7 lines 23-65); and

deciding with regard to the propagated policy and based at least in part on the responded refusal that the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same, where the media base informs the application that the particular type of action can be taken (col. 7 lines 41-65 and col. 6 lines 13-28), and the application proceeds by commanding the media base to perform such type of action (fig. 7).

Regarding claim 2, Candelore discloses the method comprising the SOTA providing the particular enabler to the application by the media base providing the application with a reference to the particular enabler (fig. 7 elements; *play content and deny enabler*).

Regarding claim 3, Candelore discloses the method comprising the interface running the enabler in an attempt to obtain the necessary data from a user of the application (fig. 7 element 706; *acquiring user rights to enable/deny access*).

Regarding claim 4, Candelore discloses the method comprising the interface running the enabler in an attempt to obtain the necessary data from one of the computing device of the application and another computing device coupled to the computing device of the application (fig. 7 element 710 and fig. 1; *downloading files to check rights access*).

Regarding claims 5 and 12, Candelore discloses the method comprising the SOTA refusing to take the action because of the lack of a proper license corresponding to the content and the interface running the enabler to obtain the proper license (col. 7 lines 9-65).

Regarding claims 6 and 13, Candelore discloses the method comprising the SOTA refusing to take the action because of the lack of a current version of an element of the protected media path and the interface running the enabler to obtain and install the current version of the element (col. 7 lines 9-65).

Regarding claims 7 and 14, Candelore discloses the method comprising the SOTA refusing to take the action because the SITA is set to be able to perform an impermissible action with respect to the content and the interface running the enabler to set the SITA to not be able to perform the impermissible action (col. 7 lines 41-54).

Regarding claim 8, Candelore discloses the method comprising the interface of the application periodically providing a progress notification to at least one of the SOTA, the application, the media base, and a user of the application (col. 7 lines 9-22 and col. 6 lines 13-28).

Regarding claims 9 and 16, Candelore discloses the method comprising the SOTA providing the particular enabler to the application from among a plurality of enablers each for responding to a particular refusal, and the interface applying a common interaction procedure to run the particular enabler where the common interaction procedure can run any of the plurality of

enablers (fig. 7).

Regarding claim 11, Candelore discloses the method comprising the SOTA providing the particular enabler to the application by the media base providing the application with a reference to the particular enabler (claim 1).

Regarding claim 15, Candelore discloses the method comprising the SOTA periodically receiving a progress notification from the interface of the application (col. 7 lines 9-22 and col. 6 lines 13-28).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

November 24, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/23/07